Oslash Private Limited

# Slice’s description of its Dr Sprinto Software Application

SprintoHQ is committed to safeguard the information and other assets shared with us by our customers, partners, and staff. They depend on us to protect their resources. Thus, it is crucial for all SprintoHQ staff to understand how to responsibly use our systems such that we can protect the security, availability and confidentiality of such assets.

## Principle & Purpose

SprintoHQ has a culture of trust and integrity. This policy aims to reinforce the trust we place in each other, by ensuring we can collectively depend on each other to protect the assets of our staff, company, partners and customers.

### Scope

This policy applies to all SprintoHQ employees, contractors, consultants, temporary, and other workers that interact with SprintoHQ systems. All such individuals are responsible for exercising good judgment to appropriately use electronic devices, data, and network resources in accordance with policies and standards, and local laws and regulation.

This policy applies to the use of

- Any company-issued electronic, computing ,storage,or network device.
- Any company owned systems on Internet/Intranet, including but not limited to servers, software, operating systems, storage, network account.
- Any company administered accounts with third party services providing email, storage, infrastructure, software, data, APIs, business systems etc, irrespective of whether such accounts

are accessed via devices owned/leased by the company, the staff member or a third party.

## Separation of concerns

SprintoHQ staff are encouraged to separate work activities from personal activities as much as possible.

SprintoHQ staff may use your company-issued devices for reasonable personal use, but those devices do not belong to you. Specifically: